4080 – Data Classification Standard:

Definition: Sensitive and Non-Sensitive Data:

Security Classifications:	There are two classifications of Data and Information Systems: 1. Sensitive 2. Non-sensitive The classification reflects the effect on the Commonwealth should that data's confidentiality, integrity, or availability be compromised. See also: • Definition: Data Security Objectives • Procedure: How to Classify Data and Systems
General Definition of Sensitive Data:	Sensitive Data are data which the unauthorized disclosure, or modification of, or disruption of use of, could cause a severe, catastrophic, or serious risk to the Commonwealth or its citizens in terms of personal safety, financial loss, identity theft, or violation of personal privacy laws.
Examples of Personal Sensitive Data:	• Federal Tax Information • Social Security Numbers • Bank Account Numbers • Credit Card Numbers • Medical Data
Examples of Commonwealth Sensitive Data	• Law Enforcement investigative data • Protective Services agency data • State/federal contracts data • Training records • Most data in State personnel records • Payroll records • Driver history records • Permits • Computer System information (e.g., network routing tables, password fields, and cryptographic key management information)
Examples of Non-sensitive Data	• Data anyone is authorized to view; appropriate for public release • Press releases • Public announcements • Publicly posted information • Posted State Office hours • Help information on completing tax returns
Examples listed are not exhaustive	The previous examples of types of data are not intended to define all the possible kinds of data used by the Commonwealth. The Agency or Cabinet data owner is responsible for classifying the data.

Definition: Data Security Objectives (from FIPS 199):

Relation to Security Classifications	In order to understand Security Classifications, we define the Security Objectives of data. How important these objectives are determines the Security Classification of the data.
Data Security Objectives	As defined in FIPS 199, there are three data security objectives: 1. Confidentiality, 2. Integrity, 3. Availability
Definition: Confidentiality Objective	Preserving authorized restrictions on information access and disclosure, including personal privacy and proprietary information.
Definition: Integrity Objective	Guarding against improper information modification or destruction, and induces ensuring information non-repudiation and authenticity.
Definition: Availability Objective	Ensuring timely and reliable access to and use of information.

Procedure: How to Classify Data and Information Systems:

<table>
<tr><td><b>Purpose</b></td><td>Different kinds of information systems require different levels of protection. Properly classifying data will assist the Commonwealth in protecting their data.
This procedure will guide you on classifying data and systems that you are responsible for. This procedure is based on FIPS 199. See also:
• Definition: Data Security Objectives
• Definition: Sensitive and Non-Sensitive Data</td></tr>
<tr><td><b>Assess Potential Impact</b></td><td>For each data security objective (Confidentiality, Integrity, and Availability), determine if the potential impact is Low, Medium, or High. Use the questions below.
What would be the level of adverse effect on operations, assets, or individuals due to:
1. the unauthorized disclosure of these data? (Confidentiality)
2. the unauthorized modification to or destruction of these data? (Integrity)
3. the disruption of access to or use of these data? (Availability)
For <i>each</i> question, and for <i>each</i> piece of data:
<table><tr><th>If the Adverse Effect is:</th><th>Then the Potential Impact is:</th></tr><tr><td>Limited</td><td>Low</td></tr><tr><td>Serious</td><td>Moderate</td></tr><tr><td>Severe or Catastrophic</td><td>High</td></tr></table></td></tr>
<tr><td><b>Assign Classification</b></td><td>If any Potential Impact is Moderate or High, then the data are classified Sensitive, else they are classified Non-Sensitive.</td></tr>
<tr><td><b>Classifying Groups of Data</b></td><td>When classifying groups of data that are used together, if any piece of data has a Potential Impact of Moderate or High, then the entire group of data is classified Sensitive.</td></tr>
<tr><td><b>Example: Classifying Groups of Data</b></td><td>A document or data record contains, among other items, a Social Security Number, The Potential Impact of disclosure of a SSN is Serious, and therefore the SSN is classified Sensitive. Because of this, the entire document or data record containing the number is also classified Sensitive, regardless of the Potential Impact of all the other items in the record.</td></tr>
<tr><td><b>Classifying Information Systems</b></td><td>1. Classify the data the System process and stores.
2. Determine the Potential Impact for the Availability Objective of the System (use the questions below)
Are any of the data stored or processed by the system classified Sensitive?
➢ If yes, then the system is classified Sensitive.
Is the Potential Impact for the Availability Objective of the System Moderate or High?
➢ If yes, then the system is classified Sensitive.</td></tr>
<tr><td><b>For Further Assistance</b></td><td>If the data owner is uncertain of the classification of a particular piece of information, the data owner should contact their manager for clarification. If an appropriate classification is still unclear, email the Information Security Office for assistance at COTSecurityAdministrationBranch@ky.gov.</td></tr>
</table>